MARCIN SARNA,
PIOTR GLEN

RODO 2018

Biuro rachunkowe musi przestrzegać przepisów o ochronie danych osobowych. Co się zmieni w 2018 roku?

FICYNA FK.
FINANSOWO-KSIĘGOWA

Autorzy: **Marcin Sarna**, radca prawny
Piotr Glen, specjalista ds. ochrony danych osobowych

Kierownik Grupy Wydawniczej: **Ewa Marmurska-Karpińska**

Wydawca: **Marta Grabowska-Peda**

Redaktor: **Katarzyna Brzozowska**

ISBN: 978-83-269-6786-3
Copyright © by Wydawnictwo Wiedza i Praktyka sp. z o.o.
Warszawa 2018

Skład i łamanie: **Raster Studio**

Wydawnictwo Wiedza i Praktyka sp. z o.o.
ul. Łotewska 9a, 03-918 Warszawa
tel. 22 518 29 29, faks 22 617 60 10

Niniejszy e-book chroniony jest prawem autorskim.
Przedruk materiałów bez zgody wydawcy jest zabroniony. Zakaz nie dotyczy cytowania publikacji z powołaniem się na źródło. Zaproponowane w niniejszym poradniku wskazówki, porady i interpretacje dotyczą sytuacji typowych. Ich zastosowanie w konkretnym przypadku może wymagać dodatkowych, pogłębionych konsultacji. Publikowane rozwiązania nie mogą być traktowane jako oficjalne stanowisko organów i urzędów państwowych.
W związku z powyższym redakcja nie może ponosić odpowiedzialności prawnej za zastosowanie zawartych w poradniku wskazówek, przykładów, informacji itp. do konkretnych przypadków.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

BIURO MUSI RESPEKTOWAĆ PRAWA OSÓB, KTÓRYCH DANE PRZETWARZA

Osoby, których dane osobowe są przetwarzane przez biuro rachunkowe, mają określone prawa. Biuro powinno je znać i respektować, gdyż za ich nieprzestrzeganie grozi grzywna, a nawet pozbawienie wolności.

Katalog uprawnień przysługujących osoba, której dane są przetwarzane, został określony ustawą o ochronie danych osobowych niezależnie od tego, przez kogo i na jakiej podstawie jej dane są przetwarzane. Zgodnie z art. 32 ust. 1 ww. ustawy osoba taka ma więc przede wszystkim:

- prawo do wniesienia sprzeciwu wobec przetwarzania jej danych w pewnych okolicznościach;
- prawo do kontroli i informacji, na które składa się prawo:
  - uzyskania wyczerpującej informacji, czy zbiór danych obejmujących jej dane w ogóle istnieje;
  - ustalenia informacji o administratorze danych (adres siedziby, nazwa);
  - uzyskania informacji o celu, zakresie i sposobie przetwarzania danych;
  - uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych;
  - uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej;
  - uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane.

WAŻNE

Ponadto osoba, której dane są przetwarzane, może zażądać:

- uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane;
- zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację.

Prawo do sprzeciwu

Zasadą jest, że aby móc przetwarzać dane osobowe, trzeba wcześniej pozyskać zgodę osoby, której one dotyczą. Od tej reguły istnieje jednak szereg wyjątków, precyzyjnie wyszczególnionych w ustawie. Zaistnienie takiego wyjątku pozwala administratorowi danych (np. biuru rachunkowemu) na przetwarzanie danych osobowych w określonych celach nawet bez tej zgody. Chodzi tu na przykład o sytuacje, gdy przetwarzanie danych jest niezbędne do:

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

- zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
- wykonania określonych prawem zadań realizowanych dla dobra publicznego;
- wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Takim usprawiedliwionym celem może być np. marketing bezpośredni własnych produktów lub usług biura rachunkowego.

Jeżeli jednak klienci biura będą zmęczeni otrzymywaniem od niego informacji handlowej (np. e-maili z propozycją rozszerzenia współpracy czy jakichś newsletterów), to mogą od takiego przetwarzania danych wnieść sprzeciw.

Uwaga

W przypadku wniesienia sprzeciwu administrator danych osobowych nie może kontynuować przetwarzania danych, a więc biuro musi zaprzestać wysyłania tych wiadomości. Nie oznacza to jednak konieczności całkowitego usunięcia danych adresata niechcianej korespondencji. Administrator ma bowiem prawo zachować dane identyfikujące jednoznacznie osobę, która zgłosiła sprzeciw (imię, nazwisko, PESEL, adres), ale wyłącznie w celu uniknięcia ponownego przetwarzania danych tej osoby.

Prawo do kontroli i informacji

Kontrolą przetwarzania danych osobowych zajmuje się Generalny Inspektor Ochrony Danych Osobowych, ale pewne uprawnienia w tym zakresie służą też samej osobie, której dane są przetwarzane. Może ona bowiem żądać informacji odnośnie do przetwarzania jej danych osobowych, czyli do biura rachunkowego może wpłynąć wniosek, w którym domaga się ona od biura informacji, czy biuro posiada jej dane osobowe. Prawo kontroli składa się z uprawnień osoby trzeciej do uzyskania informacji określonych na wstępie artykułu.

Osoba zainteresowana nie może korzystać z prawa do informacji częściej niż raz na 6 miesięcy i w takiej sytuacji biuro może odmówić przekazania wnioskowanych informacji.

Informacja o przysługujących prawach

Powyżej pisaliśmy o prawach, jakie przysługują każdemu w stosunku do administratora jego danych osobowych. Osoba taka może jednak jeszcze odpytać administratora o te prawa! Na podstawie bowiem art. 33 ustawy osoba, której dane dotyczą, może domagać się od administratora danych informacji o przysługujących jej prawach. W takiej sytuacji biuro rachunkowe będzie musiało odpowiedzieć w ciągu 30 dni.

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

Należy przestrzec przed bagatelizowaniem tego obowiązku. Jeżeli biuro nie udzieli informacji o prawach, to może to oznaczać wymierzenie na podstawie art. 54 ustawy o ochronie danych osobowych kary grzywny, kary ograniczenia wolności albo nawet pozbawienia wolności do roku.

Obowiązki administratora

Inny rodzaj korespondencji, jaka może zostać skierowana do biura rachunkowego, to pismo, którego nadawca wykazuje administratorowi danych, iż przetwarzane dane są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane. Wówczas biuro jest obowiązane do:

- uzupełnienia,
- uaktualnienia,
- sprostowania danych,
- czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru.

Czynności te administrator powinien przedsięwziąć bez zbędnej zwłoki oraz poinformować innych administratorów, którym udostępnił zbiór danych, o dokonanym uaktualnieniu lub sprostowaniu danych. W przypadku bezczynności biura osoba, której dane są przetwarzane, może zwrócić się do Generalnego Inspektora Ochrony Danych Osobowych z wnioskiem o nakazanie dopełnienia tego obowiązku.

Przepisy inne niż ustawa o ochronie danych osobowych

Uprawnienia osób, których dane są przetwarzane, regulowane są nie tylko ustawą o ochronie danych osobowych, ale także innymi przepisami. W przypadku biur rachunkowych przykładów takich sytuacji dostarczają zwłaszcza stosunki pracy pomiędzy biurem a jego pracownikami.

Pracodawca przetwarza dane osobowe pracownika, jest to bowiem niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów Kodeksu pracy. Zgodnie ze stanowiskiem Generalnego Inspektora Ochrony Danych Osobowych odcinek listy płac powinien być udostępniany w sposób uniemożliwiający wgląd do niego pozostałych współpracowników, a pracodawca jest zobowiązany chronić te dane w sposób szczególny. Artykuł 26 ust. 1 ustawy nakazuje administratorowi danych dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą.

PRZYKŁAD

Biuro rachunkowe jest prowadzone w formie spółki z ograniczoną odpowiedzialnością, a wspólnik tej spółki chce uzyskać dostęp do listy płac pracowników biura. Jako podstawę prawną swojego żądania powołuje art. 212 Kodeksu spółek handlowych, zgodnie z którym prawo kontroli służy każdemu wspólnikowi i w tym celu wspólnik lub wspólnik

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

z upoważnioną przez siebie osobą może w każdym czasie przeglądać księgi i dokumenty spółki, sporządzać bilans dla swego użytku lub żądać wyjaśnień od zarządu.

Przepis wydaje się brzmieć kategorycznie i nakazywać ujawnienie wspólnikowi biura informacji o zarobkach jego pracowników. Tymczasem analizowana norma prawna wcale nie kreuje bezwzględnego prawa żądania informacji o spółce, a wręcz przeciwnie – doznaje ograniczeń wynikających z regulacji szczególnych, w tym właśnie z ustawy o ochronie danych osobowych. Informacje na temat wysokości wynagrodzenia konkretnego pracownika są danymi osobowymi w rozumieniu tej ustawy.

Z tych też powodów biuro (spółka, administrator danych) nie może ujawnić osobom trzecim (a takimi są wobec pracodawcy i pracownika wspólnicy spółki) wysokości wynagrodzenia pracownika bez jego zgody. Ujawnienie tych informacji stanowiłoby naruszenie danych osobowych pracownika biura. Może on wówczas domagać się od pracodawcy zadośćuczynienia i odszkodowania. Niezależnie od powyższego w grę wchodzi także kwestia naruszenia dóbr osobistych (art. 23 i 24 Kodeksu cywilnego), na co zwrócił uwagę Sąd Najwyższy w uchwale z 16 lipca 1993 r. (sygn. akt I PZP 28/93).

Oznacza to, że zakres uprawnień osoby, której dane są przetwarzane, wykracza poza uprawnienia z samej ustawy o ochronie danych osobowych i obejmuje także uprawnienia wynikające chociażby z przepisów Kodeksu cywilnego (odszkodowanie).

PRZYKŁAD

Pracodawca stosuje monitoring wizyjny pracownika (np. zamontowanie kamery nad stanowiskiem pracy). Monitorowanie pracowników nie narusza ich dóbr osobistych i jest uznane za dopuszczalne, jeżeli pracownicy zostali o tym poinformowani (z wyjątkiem uzasadnionych podejrzeń o naruszenie prawa, np. notorycznego dopuszczania się przez pracowników kradzieży). Celem tego działania jest ochrona słusznego interesu pracodawcy, a przyjęta forma i zakres monitoringu są do tego celu proporcjonalne. Zainstalowanie kamery nie wymaga przy tym uzyskania zgody pracowników, jak też reprezentujących ich interesy organizacji związkowej.

§ Podstawa prawna:

- art. 32 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn:. Dz.U. z 2015 r. poz. 2135 ze zm.).

Marcin Sarna
radca prawny

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

SPRAWDŹ, JAK WŁAŚCIWIE ZABEZPIECZYĆ DANE SWOICH KLIENTÓW

Przetwarzając dane osobowe klientów, prowadząc zbiory danych na cele marketingowe, a wreszcie dysponując danymi osobowymi osób trzecich, biuro rachunkowe musi dbać o właściwe ich zabezpieczenie. Zobacz, jakie środki możesz w tym celu zastosować.

Powierzone lub zebrane dane trzeba zabezpieczyć

Dane osobowe otrzymane przez biuro rachunkowe od swoich klientów powinny być przez to biuro przetwarzane na podstawie umowy powierzenia przetwarzania danych osobowych zawartej przez biuro z klientem. Wówczas wprawdzie administratorem danych osobowych pozostaje klient ale biuro w zakresie zabezpieczania danych osobowych ponosi odpowiedzialność dokładnie tak samo surową jak administrator danych. Drugą kategorią danych osobowych przetwarzanych przez biuro są dane, które nie pochodzą od osoby trzeciej (biuro samo je zbiera i tworzy zbiory danych). W tym zakresie biuro jest administratorem danych osobowych i także musi je zabezpieczyć.

WAŻNE

Zabezpieczenie danych osobowych może mieć charakter:

- prawny – regulacje obowiązujące u administratora danych osobowych, np. polityka prywatności, instrukcja zarządzania systemem informatycznym;
- organizacyjny – takie rozwiązania administracyjne (techniczne) jak polityka kluczy, zmiany haseł, udzielania i cofania upoważnień do przetwarzania danych;
- informatyczny – środki elektroniczne służące zachowaniu bezpieczeństwa i integralności przetwarzanych danych takie jak firewalle, oprogramowanie antywirusowe, infrastruktura sieciowa, system wykrywania naruszeń;
- fizyczny.

Ważna jest odpowiednia dokumentacja

Niektóre środki zabezpieczające dane osobowe powinny być poczynione zanim dojdzie do przetwarzania danych osobowych. Biuro powinno mieć bowiem m.in. wdrożoną dokumentację dotyczącą zabezpieczenia danych osobowych. Administrator danych osobowych albo administrator bezpieczeństwa informacji (jeżeli został powołany w danym biurze) jest zobowiązany do nadzorowania opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

W skład tej dokumentacji wchodzą dokumenty wskazane w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Jest to:

1) polityka bezpieczeństwa;
2) instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

W polityce bezpieczeństwa nie reguluje się konkretnych kwestii technicznych – to znajdziemy w instrukcji zarządzania systemem informatycznym. Jest to natomiast zestaw reguł prawnych i praktycznych zasad regulujących sposób przetwarzania danych wewnątrz organizacji. Celem istnienia polityki jest po prostu wskazanie czynności niezbędnych do tego, aby administrator danych należycie wykonywał swoje obowiązki w zakresie zabezpieczenia danych, które posiada.

Instrukcja zarządzania systemem informatycznym ma z kolei za zadanie uzupełniać politykę bezpieczeństwa w zakresie technicznych aspektów przetwarzania danych. W praktyce składa się ona z wielu odrębnych dokumentów (załączników do instrukcji), różnych w zależności od wielkości danego administratora danych (biura rachunkowego). Może to być np.:

1) instrukcja postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych;
2) ewidencja osób upoważnionych do przetwarzania danych osobowych;
3) wykaz budynków i pomieszczeń, gdzie przetwarza się dane osobowe;
4) wykaz systemów i programów używanych do przetwarzania danych osobowych;
5) wzór upoważnienia do przetwarzania danych osobowych – aby konkretny pracownik biura rachunkowego miał możliwość operowania na danych osobowych powinien być do tego upoważniony przez administratora danych (kierownictwo biura);
6) wzór oświadczenia o zobowiązaniu się do zachowania w tajemnicy danych osobowych – podpisywane przez każdego nowoprzyjętego pracownika biura rachunkowego;
7) wzór umowy powierzenia przetwarzania danych osobowych – w celu ustandaryzowania treści takich umów zawieranych przez biuro rachunkowe z klientami.

Zbiory należy zgłosić do GIODO

W przypadku danych osobowych tworzących pewien odpowiednio uporządkowany zestaw, gdy dostęp do konkretnych danych w ramach tego zestawu jest możliwy według określonych kryteriów, mamy do czynienia ze zbiorem danych osobowych. Zbiór powinien być zgłoszony do rejestracji u Generalnego Inspektora Ochrony Danych Osobowych. Istnieją jednak wyjątki od tej reguły ze względu na charakter zbiorów i cele przetwarzania danych

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

oraz ze względu na potrzebę ochrony interesu publicznego. Z obowiązku rejestracji zbioru danych biuro rachunkowe będzie więc zwolnione np. w przypadku danych przetwarzanych:

1) w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się;
2) wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej;
3) w zakresie drobnych bieżących spraw życia codziennego.

Niezbędny jest administrator bezpieczeństwa informacji

Administrator bezpieczeństwa informacji to kluczowa postać w procesie ochrony danych osobowych. ABI powołuje administrator danych osobowych, czyli na przykład zarząd spółki prowadzącej biuro rachunkowe. Zawsze jednak ABI powinien zostać tak uplasowany w strukturze organizacyjnej danego podmiotu, aby podlegał bezpośrednio kierownikowi tej jednostki (tj. w tym przykładzie – zarządowi).

Uwaga

Decyzja o powołaniu ABI należy do administratora danych osobowych, który – jeżeli stwierdzi, że potrafi samodzielnie zapewnić prawidłowe przetwarzanie danych osobowych – nie musi wyznaczać ABI.

Główną zaletę płynącą z powołania ABI stanowi zwolnienie administratora danych z obowiązku rejestrowania u GIODO zbiorów przetwarzanych przez niego danych osobowych. Gdy więc w biurze jest ABI, to danego zbioru danych podlegającego obowiązkowi zgłoszenia do GIODO nie trzeba zgłaszać do GIODO, a wystarczy zarejestrować go u ABI w danym biurze. Poza tym zarząd biura nie musi się na bieżąco zajmować zabezpieczaniem danych osobowych w spółce, bo ma do tej pracy właśnie ABI.

Do przetwarzania danych niezbędne jest upoważnienie

Jak już wspominaliśmy, aby pracownik mógł zostać dopuszczony do przetwarzania danych osobowych, powinien posiadać upoważnienie do ich przetwarzania, a wzór tego upoważnienia może stanowić element instrukcji zarządzania systemem informatycznym. Pamiętajmy przy tym, że przetwarzanie danych to bardzo szerokie pojęcie oznaczające wszelkie operacje wykonywane na danych osobowych. Chodzi tu więc np. o zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie czy usuwanie. Administrator danych powinien też prowadzić ewidencję osób, które zostały upoważnione do przetwarzania danych osobowych. Z ewidencji powinno wynikać, kto (imię, nazwisko), od kiedy, do kiedy i w jakim zakresie został upoważniony do przetwarzania danych osobowych.

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

Pomyśl o fizycznym zabezpieczeniu danych i systemów informatycznych

Zabezpieczenie fizyczne danych osobowych to wszelkie materialne środki służące ochronie danych osobowych, mające na celu utrudnić lub uniemożliwić dostęp do danych osobom nieuprawnionym, np. ogrodzenie, sejf, ale również monitoring, czujki ruchu, alarm przeciwwłamaniowy.

Artykuły 36-39 ustawy o ochronie danych osobowych, które regulują zabezpieczanie danych, nie precyzują, jakie fizyczne środki ochrony danych powinny być przedsiębrane w konkretnym przypadku. Biuro samo musi ocenić, jakich środków ochrony fizycznej potrzebuje, aby skutecznie ograniczyć i kontrolować dostęp do przetwarzanych danych, biorąc pod uwagę rodzaj przetwarzanych danych.
Jeśli chodzi o wymogi techniczne i organizacyjne zabezpieczania systemów informatycznych w polityce bezpieczeństwa, należy zamieścić następujące informacje mające związek z fizycznym zabezpieczaniem danych:

- wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
- określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Z kolei w instrukcji zarządzania systemem informatycznym reguluje się sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych.
Aby ochrona fizyczna była skuteczna, powinniśmy uniemożliwić dostęp osobom nieuprawnionym do elementów systemów i sieci teleinformatycznych.

Tu pomóc może system kontroli dostępu, a w jego ramach – jednoznaczny (konkretny) podział obiektu (np. budynku) na strefy zabezpieczające. Strefy te można podzielić na strefy zastrzeżone, strefy szczególnie chronione i strefy z ograniczonym dostępem. Do zabezpieczania dostępu do pomieszczeń oraz kontroli wejść i wyjść służą bramki, liczniki, zamki szyfrowe czy zabezpieczenia biometryczne.

§ Podstawa prawna:

- rozporządzenie ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,
- art. 36–39 ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz.U. z 2015 r. poz. 2135 ze zm.).

Marcin Sarna
radca prawny

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

PAMIĘTAJ O PODPISANIU Z KLIENTEM UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Procesorem jest podmiot, który przetwarza dane osobowe w imieniu administratora. Jest nim też biuro rachunkowe. Jeżeli więc administrator danych zleca podmiotowi zewnętrznemu przetwarzanie danych, za które odpowiada, jest to powierzenie danych do przetwarzania, które powinno być regulowane umową. Sprawdź, na co powinieneś zwrócić uwagę.

Podmiot, któremu powierzono dane do przetwarzania, nie jest ich administratorem, nie decyduje, co można z tymi danymi zrobić, nie może ich wykorzystywać do własnych celów. Jest to procesor, który realizuje zadania i cele określone przez administratora danych. Biuro rachunkowe więc jest najczęściej procesorem, bo są mu powierzane dane z innych firm współpracujących z biurem, na przykład w zakresie obsługi księgowo-kadrowej.

To te firmy są administratorami danych, a powierzają do zewnętrznego biura rachunkowego dane czy towoich pracowników, czy dotyczące transakcji, w celu realizacji odpowiednich usług.

WAŻNE

Administrator danych może powierzyć innemu podmiotowi przetwarzanie danych, ale w drodze umowy zawartej na piśmie. Podmiot przetwarzający (procesor) może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie (art. 31 ustawy o ochronie danych osobowych).

Na często więc padające pytanie, czy pracodawca zlecający podmiotowi zewnętrznemu prowadzenie obsługi księgowej ma również obowiązek zawarcia z nim umowy powierzenia przetwarzania danych osobowych, należy odpowiedzieć twierdząco. Tak, ma taki obowiązek, gdyż wynika to z ustawy o ochronie danych osobowych, a prowadzenie dokumentacji księgowej wiąże się nierozerwalnie z przetwarzaniem danych osobowych pracowników. Pracodawca udostępniając dane osobowe pracowników podmiotowi zewnętrznemu w celu prowadzenia obsługi księgowej swojej dokumentacji, ma obowiązek zawrzeć z nim odrębną umowę powierzenia danych osobowych. Często bowiem pracodawca mylnie uważa, że skoro udzielił podmiotowi zewnętrznemu pełnomocnictwa do jego reprezentowania (np. przed urzędem skarbowym i Zakładem Ubezpieczeń Społecznych) we wszystkich sprawach związanych z prowadzeniem księgowości, to pełnomocnictwo to stanowi podstawę powierzenia przetwarzania danych osobowych. Jest to sprzeczne z ustawą o ochronie danych osobowych, gdyż jej przepisy wyraźnie wymagają, aby umowa powierzenia przetwarzania danych osobowych była odrębną umową.

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

Zapisy w umowie powinny określać co najmniej cel powierzenia, zakres powierzonych danych, zakres czynności wykonywanych na danych, zakres odpowiedzialności procesora, możliwość kontroli przez administratora, sposób postepowania z danymi po wygaśnięciu umowy.

Umowa powierzenia powinna wymagać od procesora stosowania odpowiednich środków bezpieczeństwa dla ochrony powierzonych danych. O umowie powierzenia powinien pamiętać administrator danych. Coraz częściej jednak to już biura rachunkowe, zdające sobie sprawę z tych obowiązków, mają odpowiednie wzory umów, wraz z zapisami lub załącznikami określającymi zasady powierzenia danych. Podnosi to jeszcze bardziej wiarygodność i profesjonalizm biura.

Biuro rachunkowe, zarówno jako administrator danych, jak i procesor, zobowiązane jest zastosować odpowiednie środki bezpieczeństwa i przestrzegać zasad i przepisów dotyczących ochrony danych. Generalnie za bezpieczeństwo swoich danych zawsze odpowiada administrator, ale nie wyłącza to odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową. Jeszcze bardziej rygorystycznie reguluje te kwestie ogólne rozporządzenie UE o ochronie danych (RODO), mające obowiązywać od maja 2018 roku.

WAŻNE

Ewentualnie odpowiednie zapisy regulujące kwestie powierzenia przetwarzania danych powinny być zawarte w umowie głównej na obsługę.

Po zakończeniu przetwarzania w imieniu administratora podmiot przetwarzający powinien – zgodnie z decyzją administratora – zwrócić lub usunąć dane osobowe, chyba że prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający, nakładają obowiązek przechowywania danych osobowych. Bezwzględnie więc biura rachunkowe, chcąc zapewnić gwarancję odpowiedniej ochrony dla przetwarzanych danych, muszą zarówno formalnie, jak i przede wszystkim praktycznie, spełniać wymogi organizacyjno-techniczne zalecane przepisami prawa, a także dobrymi, sprawdzonymi praktykami. To wszystko i jako administrator danych, i jako procesor, zwłaszcza że w obu przypadkach odpowiedzialność jest bardzo duża.

Piotr Glen
specjalista ds. ochrony danych osobowych

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

PAMIĘTAJ O ZOBOWIĄZANIU SWOICH PRACOWNIKÓW DO ZACHOWANIA POUFNOŚCI

Pracownicy biura rachunkowego przetwarzający dane osobowe, powierzone przez klientów biura, powinni mieć do tych czynności odpowiednie upoważnienia. Pobierz wzór upoważnienia i sprawdź zasady jego sporządzania.

Przepisy narzucają na administratora danych obowiązek zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru, do bazy, do systemu wprowadzone oraz komu są przekazywane. Właściciel biura rachunkowego, jako administrator danych, oprócz tego, że musi wiedzieć, kto u niego pracuje, kto do jakich danych ma dostęp i jakie operacje może na nich wykonywać, musi również w odpowiedni sposób upoważnić swoich pracowników i współpracowników do przetwarzania danych osobowych.

Należy pamiętać, że taką osobą upoważnioną do przetwarzania danych będzie ktoś, kto wykonując swoje służbowe obowiązki, ma dostęp do określonych danych. Będzie to więc pracownik zatrudniony na stanowisku związanym z przetwarzaniem danych, osoba zatrudniona na umowę o dzieło czy zlecenie, jeśli jej wykonywane usługi polegają na dostępie do danych osobowych, czy nawet praktykant lub stażysta, którego na przykład zadaniem będzie skanowanie umów. Nie będzie natomiast osobą upoważnioną do przetwarzania danych osobowych np. sprzątaczka. Z jej obowiązków służbowych nie wynika możliwość oficjalnego dostępu do danych. Nieoficjalnie też taka osoba nie może niczego, co stanowi tajemnicę danych osobowych czy tajemnicę przedsiębiorstwa, zobaczyć. O tym muszą pamiętać osoby upoważnione do przetwarzania danych i między innymi stosować się do zasady „czystego biurka”.

UWAGA

Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia (art. 39 ust. 2 ustawy o ochronie danych osobowych). Dlatego należy stosować upoważnienia wraz z zobowiązaniem do zachowania tajemnicy danych osobowych i do przestrzegania zasad i przepisów dotyczących ochrony danych. Wtedy również i osoba upoważniona odpowiada za bezpieczeństwo danych.

Upoważnienia do przetwarzania danych nadaje administrator danych, ale to nie znaczy, że osobiście musi to robić właściciel czy prezes. Zależy to od wewnętrznej organizacji, procedur i pełnomocnictw w danej firmie. Zapewne w każdym biurze proces zatrudniania, jak również zakończenia zatrudnienia odbywa się w sposób zorganizowany i uwzględnia zasady

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

bezpieczeństwa informacji. W każdym razie czy to w opisie stanowiska pracy, czy w warunkach zatrudnienia, czy w umowie, czy właśnie w upoważnieniu do przetwarzania danych należy zawrzeć wymagania i odpowiedzialność związaną z bezpieczeństwem i ochroną danych oraz określić zakres uprawnień co do przetwarzania danych osobowych, jeżeli wykonywana praca związana jest z dostępem do danych osobowych.

WAŻNE

Forma upoważnienia do przetwarzania danych osobowych nie jest w żaden sposób określona i może być różna, tak jak i sposób, i organizacja ich wydawania.

Inaczej mogą być nadawane upoważnienia w dużej korporacji zatrudniającej tysiące pracowników, zatrudnionych dodatkowo w wielu terenowych oddziałach, a inaczej w małej czy średniej firmie. Czy będzie to odrębny dokument, czy załącznik do umowy o pracę, czy zakres uprawnień i odpowiedzialności opisany w zakresie obowiązków, to zależy od pracodawcy i jego organizacji pracy. Upoważnienia do przetwarzania danych powinny więc być wydawane (podpisywane) przez pracodawcę jako administratora danych lub przez osoby, które posiadają stosowne pełnomocnictwo wydane przez pracodawcę. Generalnie musi być to czynność prawna. Nie może więc być mowy o słownych upoważnieniach.

Podkreślić należy, że każde biuro rachunkowe, jako administrator danych, musi wywiązać się ze wszystkich organizacyjnych i technicznych obowiązków, jakie narzucają przepisy prawa dotyczące przetwarzania i ochrony danych osobowych.
Zgodnie z art. 36 uodo (ustawy o ochronie danych osobowych) administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator danych ma prowadzić dokumentację opisującą sposób przetwarzania danych oraz zastosowane środki dla ich ochrony. Na taką dokumentację składa się przede wszystkim polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Z takich głównych dokumentów wynikają natomiast kolejne, szczegółowe instrukcje i procedury.

Sposób i forma prowadzenia takiej ewidencji i wskazanie osoby za to odpowiedzialnej zależą od wewnętrznych ustaleń firmy (administratora danych). Wprawdzie mające niebawem obowiązywać unijne rozporządzenie o ochronie danych osobowych (rodo) nie narzuca tak szczegółowych regulacji i wprost nie nakazuje prowadzenia w pisemnej formie tylu dokumentów opisujących zasady ochrony danych wdrożone u administratora danych, niemniej powinność i odpowiedzialność dotycząca zapewnienia bezpieczeństwa danych osobowych będzie jesz-

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

cze większa. Dotychczasowe więc procedury, w praktyczny, rozsądny i zrozumiały sposób wdrożone w ramach polityki bezpieczeństwa informacji, nadal będą miały zastosowanie i będą dowodem na należyty nadzór nad realizacją przepisów prawa.

UWAGA

Administrator danych zobowiązany jest prowadzić między innymi ewidencję osób upoważnionych do przetwarzania danych, która musi zawierać imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, identyfikator (login), jeżeli dane są przetwarzane w systemie informatycznym (art. 39 ust. 1 uodo).

Tym samym zawsze do przetwarzania danych będą mogły być dopuszczone jedynie osoby upoważnione, przeszkolone z zasad ochrony danych i zobowiązane do zachowania tajemnicy danych osobowych.

Wszyscy pracownicy i współpracownicy powinni być świadomi swoich obowiązków i odpowiedzialności prawnej oraz zagrożeń związanych z bezpieczeństwem informacji. W tym celu należy zapewnić wszystkim pracownikom i współpracownikom właściwy poziom świadomości poprzez kształcenie i szkolenie z zakresu bezpieczeństwa informacji, ze szczególnym uwzględnieniem procedur bezpieczeństwa wynikających z przepisów i wewnętrznych zasad wdrożonych do stosowania u administratora danych.

WAŻNE

Zgodnie z aktualnymi przepisami ustawy o ochronie danych osobowych szkolenie w tym zakresie, a przynajmniej zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych, jest obowiązkowe. Forma szkolenia nie jest określona, ale należy takowe zorganizować i mieć jakieś potwierdzenie przeszkolenia osób przetwarzających dane. Pamiętajmy o tym, zatrudniając nowych pracowników czy też przygotowując stażystów lub praktykantów.

Nowo zatrudniona osoba, zanim otrzyma określone uprawnienia, zwłaszcza w systemie informatycznym służącym do przetwarzania danych, powinna otrzymać w jakiejś formie upoważnienie do przetwarzania danych osobowych, poprzedzone jej oświadczeniem, że zna i stosuje się do zasad i przepisów z zakresu ochrony danych osobowych. Tym samym z tymi przepisami i zasadami powinna być zapoznana i najlepiej w skuteczny, przystępny, zrozumiały i praktyczny sposób być przeszkolona w tym zakresie. Wspomnę tu, że nie jest najlepszym rozwiązaniem odesłać pracownika do ustawy o ochronie danych osobowych czy nawet wewnętrznej polityki bezpieczeństwa, aby jedynie przeczytał te dokumenty. Warto mimo wszystko organizować w jakiejś formie w miarę regularne szkolenia z praktycznych aspektów ochrony danych, zarówno

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

dla nowych, jak i wcześniej zatrudnionych pracowników. Zwłaszcza że przepisy dotyczące przetwarzania i ochrony danych dość dynamicznie się zmieniają. Pojawiają się też raz po raz nowe zagrożenia i metody wykradania danych.

Dane osobowe mają dużą wartość. Dlatego też klienci biur rachunkowych, tj. przedsiębiorcy zlecający obsługę kadrowo-księgową, powinni wymagać i najczęściej już to robią, aby biuro podpisało odpowiednią umowę powierzenia przetwarzania danych, która będzie gwarantować klientowi odpowiedni poziom ochrony dla powierzanych do biura danych. To w takiej umowie klient zapewnia sobie, że do danych przekazanych do biura będą miały dostęp jedynie osoby upoważnione, zobowiązane do zachowania tajemnicy i poufności. W takiej sytuacji biuro rachunkowe jest tzw. procesorem, podmiotem przetwarzającym dane, odpowiadającym na równi z klientem, jako administratorem danych, za bezpieczeństwo przyjętych do przetwarzania danych osobowych.

Należy w tym miejscu podkreślić, że klient nie upoważnia pracowników biura do przetwarzania danych, jakie w ramach umowy przekazuje. To nie klient, nie zleceniodawca nadaje upoważnienia pracownikom zewnętrznego biura. Biuro, zarówno jako administrator danych, jak i jako procesor, gwarantuje klientom, że do przetwarzania danych osobowych dopuszcza jedynie osoby odpowiednio upoważnione przez biuro, które są przeszkolone i zobowiązane do zachowania tajemnicy. Tak więc proces nadawania upoważnień do przetwarzania danych osobowych, procedury przyznawania, a zwłaszcza odbierania uprawnień w systemach informatycznych służących do przetwarzania danych, oświadczenia o zachowaniu tajemnicy danych osobowych, zachowanie w poufności informacji objętych prawem tajemnicy przedsiębiorstwa, mają bardzo duże znaczenie nie tylko ze względu na formalne, ustawowe wymogi w tym zakresie, ale przede wszystkim dla praktycznego, biznesowego bezpieczeństwa. Powinno mieć to szczególne zastosowanie dla pracowników i współpracowników biur rachunkowych, którzy mają dostęp do bardzo wielu i różnych informacji i danych osobowych, oczywiście w stopniu niezbędnym do wykonania swoich obowiązków.

Piotr Glen
specjalista ds. ochrony danych osobowych

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

RODO. POZNAJ NOWE REGULACJE W ZAKRESIE OCHRONY DANYCH OSOBOWYCH PRACOWNIKÓW

Nowe rozporządzenie europejskie dotyczące ochrony danych osobowych (tzw. RODO) wprowadzi już niedługo prawdziwą rewolucję. W pewnym zakresie zmiany dotkną także pracodawców przetwarzających dane osobowe pracowników. Jeżeli więc Twoje biuro zatrudnia pracowników albo też ma dostęp do danych osobowych pracowników zatrudnionych w zewnętrznych firmach lub takie dane przekazuje – koniecznie zapoznaj się ze zmianami.

W dniu 14 kwietnia 2016 r. zostało przyjęte rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Jest to tzw. ogólne rozporządzenie o ochronie danych osobowych, w skrócie właśnie RODO.

Jako cel rozporządzenia wskazano zapewnienie wysokiego i ujednoliconego poziomu ochrony danych w całej Unii Europejskiej oraz silniejszą (niż do tej pory), a także dostosowaną do wymogów epoki cyfrowej ochronę praw konsumentów i konkurencji.

UWAGA

Nowe zasady wejdą w życie dwa lata po opublikowaniu rozporządzenia, tj. 25 maja 2018 r., ale już dziś warto zacząć przygotowania do ich stosowania.

Zmiany, które powinny zainteresować pracodawców i pracowników

Rozporządzenie reguluje m.in. następujące kwestie mające znaczenie dla ochrony danych osobowych pracowników przez pracodawców:

- ochronę danych osobowych w grupie kapitałowej;
- obowiązek ustanowienia inspektora ochrony danych osobowych;
- warunki wyrażenia zgody na przetwarzanie danych prywatnych;
- prawo do przenoszenia danych do innego usługodawcy;
- nakładanie administracyjnych kar pieniężnych (do 4% całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego) i ich skuteczne egzekwowanie.

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

Biuro rachunkowe funkcjonujące w ramach grupy przedsiębiorstw

W rozporządzeniu znajduje się nowa regulacja dotycząca przetwarzania danych osobowych w grupie kapitałowej. Ta grupa kapitałowa jest zwana „grupą przedsiębiorstw". Grupą przedsiębiorstw w rozumieniu rozporządzenia jest bowiem przedsiębiorstwo kontrolujące przetwarzanie danych osobowych w przedsiębiorstwach powiązanych z nim, wraz z tymi przedsiębiorstwami. Grupą przedsiębiorstwa zarządza główna jednostka organizacyjna.

Jeżeli biuro rachunkowe jest jedną ze spółek wchodzących w skład grupy kapitałowej (a tak może być na przykład w przypadku tzw. centrum usług wspólnych), to grupa może wyznaczyć jednego inspektora ochrony danych dla wszystkich przedsiębiorstw.
Jeżeli grupa jest międzynarodowa, to może wybrać jeden państwowy organ ochrony danych osobowych (np. polskiego GIODO) dla wszystkich przedsiębiorstw grupy (tzw. *one-stop-shop*).

Zapisy te mają znaczenie także dla biur rachunkowych, które nie są członkami grupy kapitałowej, ale obsługują spółkę lub spółki takiej grupy. Wówczas, w przypadku powierzenia biuru danych osobowych pracowników spółek grupy kapitałowej, należy poznać i stosować zasady przetwarzania danych w danej grupie.

Inspektor ochrony danych

Tytułowy termin oznacza tak naprawdę „starego" administratora bezpieczeństwa informacji. Zupełnie inaczej niż do tej pory sprecyzowano natomiast przesłanki obowiązku jego ustanowienia. W Twoim biurze obowiązek powołania inspektora ochrony danych będzie obowiązywał tylko jeżeli biuro jest administratorem danych osobowych:

- którego główna działalność polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;
- którego główna działalność polega na przetwarzaniu na dużą skalę danych osobowych.

UWAGA

Inspektor ochrony danych może być członkiem personelu biura lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług. Jego dane muszą być opublikowane przez administratora.

Wydaje się więc, że w większości przypadków typowe biura rachunkowe nie będą musiały mieć inspektora ochrony danych. Inaczej będzie, jeżeli biuro wykonuje np. także zadania z zakresu obsługi typowo kadrowej i na dużą skalę albo świadczy usługi polegające na monitorowaniu działań pracowników.

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

Warunki wyrażenia zgody na przetwarzanie danych osobowych

Spośród wielu nowości wyróżnia się także sama forma wyrażenia zgody: ma ona być udzielona w formie oświadczenia lub wyraźnego działania, stanowiących przejaw dobrowolnego, konkretnego, świadomego i jednoznacznego przejawu woli, potwierdzającego przyzwolenie na przetwarzanie przez podmiot danych osobowych.

Zgody w takiej formie biuro będzie musiało zażądać od osób zatrudnionych w biurze niepracowniczo (np. na umowie zlecenia czy umowie o dzieło) w każdym przypadku, gdy zajdzie potrzeba przetwarzania danych osobowych takich osób w celach innych niż wykonanie umowy.

Co więcej, takiej wyraźnej, osobnej zgody wymagać będzie także tzw. profilowanie. Chodzi tu o zautomatyzowane przetwarzanie danych osobowych w celu oceny niektórych czynników osobowych osoby fizycznej, np. do analizy lub prognozy sytuacji ekonomicznej, zdrowia czy osobistych preferencji danej osoby. Przykładem może tu być gromadzenie takich danych o klientach biura w celu dostosowania oferty marketingowej biura do potrzeb rynku.

Powierzenie danych

Biura rachunkowe bardzo często w swojej pracy posługują się podwykonawcami czy innymi podmiotami, z którymi stale lub okresowo współpracują, np. informatykami, windykatorami czy prawnikami. Aby podmioty te mogły prawidłowo wykonywać swoje obowiązki, bardzo często muszą mieć dostęp do danych osobowych pracowników biura czy pracowników klienta biura. W związku z powyższym już w obecnym stanie prawnym istnieje konieczność powierzenia przez administratora (biuro rachunkowe) posiadanych przez niego danych osobowych w drodze umowy. Podmioty, którym te dane biuro powierzyło do przetwarzania, zwane są procesorami.

WAŻNE

Umowa powierzenia powinna być obecnie i będzie mogła być nadal zawarta w formie pisemnej. Rozporządzenie wyraźnie dopuszcza także formę elektroniczną.

Do tej pory umowa miała zawierać jedynie zakres i cel przetwarzania danych osobowych. Po wejściu w życie nowych regulacji umowa powinna określać:

- przedmiot i czas trwania przetwarzania,
- charakter i cel przetwarzania,
- rodzaj danych osobowych,
- kategorie osób, których dane dotyczą,
- obowiązki i prawa administratora,
- obowiązki procesora.

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

Trzeba przy tym zaznaczyć, że rozbudowanie w rozporządzeniu elementów umowy o powierzenie przetwarzania nie wprowadza rewolucji, gdyż już obecnie dobrze skonstruowana umowa powierzenia powinna te elementy zawierać.

A co w przypadku gdy np. informatyk zechce powierzyć dane osobowe powierzone mu przez biuro, np. gdy musi zatrudnić inną firmę informatyczną w charakterze podwykonawcy? Obecnie ustawa nie reguluje w ogóle kwestii tego tzw. podpowierzenia. Natomiast rozporządzenie przewiduje obowiązek procesora uzyskania pisemnej zgody administratora danych na przekazanie tych danych innemu podmiotowi (czyli zgody na podpowierzenie).

Taka zgoda może na szczęście być wyrażona przez biuro ogólnie, tj. nie na każdego podwykonawcę z osobna, ale np. w taki sposób: „Twoja rachunkowość sp. z o.o. (administrator danych) zgadza się na przekazywanie przez ABC Informatyka S.A. (wykonawca) podwykonawcom zaangażowanym w związku z obsługą informatyczną administratora danych, wszystkich danych osobowych przekazanych przez administratora danych wykonawcy na podstawie umowy powierzenia danych osobowych z 12 marca 2017 r.”.

Inne zmiany merytoryczne

Biuro rachunkowe przetwarzające dane osobowe swoich pracowników musi też pamiętać, że rozporządzenie poszerza katalog danych wrażliwych o dane genetyczne i biometryczne. Oznacza to konieczność szczególnej ochrony danych osobowych pracowników w przypadku np. limitowania dostępu do pomieszczeń lub ewidencji czasu pracy z wykorzystaniem czytników odcisku palca albo siatkówki oka.

Innym *novum* jest też:

- *privacy by design* – obowiązek uwzględniania zagadnień ochrony danych już na etapie projektowania rozwiązań, np. w przypadku zamawiania systemu informatycznego powinien on od początku spełniać wymogi ochrony danych osobowych;
- *privacy by default* – system informatyczny ma domyślnie przetwarzać dane osobowe w minimalnym (niezbędnym) zakresie, np. system informatyczny biura nie powinien przetwarzać danych osobowych pracownika w zakresie wynagrodzenia, gdy jego wyłącznym zadaniem jest zarządzanie czasem pracy, w tym urlopami. Dane o czasie pracy, które mają znaczenie dla wynagrodzenia, powinny być przekazywane do systemu płacowego. Pozwoli to na wyeliminowanie ryzyka, że dane o wynagrodzeniu pracownika będą przetwarzane przez pracownika biura odpowiedzialnego za urlopy (np. bezpośredniego przełożonego), a nie przez wyłącznie odpowiedzialne w tym zakresie służby finansowo-księgowe.

Marcin Sarna
radca prawny

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

POZNAJ 4 WSKAZÓWKI DOTYCZĄCE OBOWIĄZKÓW BIURA JAKO ADMINISTRATORA I PROCESORA

Określając obowiązki administratorów danych, zarówno w świetle obecnych, jak i przyszłych przepisów prawa, warto zwrócić uwagę na wskazówki prezentowane poniżej, dotyczące małych i średnich biur rachunkowych. Mogą być one stosowane również w rozbudowanych organizacjach, w dużych korporacjach i spółkach, po ich uszczegółowieniu.

Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych (art. 36 ust. 2 uodo).

Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki bezpieczeństwa obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.
Stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonego mechanizmu certyfikacji może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków (art. 24 ust. 2 i 3 RODO).

Wskazówka

Biuro rachunkowe powinno opracować i wdrożyć Politykę bezpieczeństwa informacji ze szczególnym uwzględnieniem ochrony danych osobowych. Dokument Polityki bezpieczeństwa danych osobowych powinien określać podstawy prawne przetwarzania danych w danej organizacji, zakres danych (kategorie danych) objętych ochroną, zasady dopuszczenia osób do przetwarzania danych osobowych – nadawanie upoważnień, zasady powierzania i udostępniania danych, zasady ochrony obszaru przetwarzania danych, zasady monitorowania ochrony danych, zasady przetwarzania danych w systemie IT oraz na nośnikach papierowych i elektronicznych – odniesienie do Instrukcji zarządzania systemem informatycznym, zasady archiwizacji danych i przechowywania kopii zapasowych, zasady postępowania w sytuacji naruszenia zasad ochrony danych, odpowiedzialność prawną za naruszenia zasad ochrony danych. Dokument główny może być zbiorem ogólnych zasad i wytycznych. Szczegóły warto opisać w załącznikach do Polityki. Wzory pomocnych załączników przedstawione są na www.dokumentacjaksiegowa.pl.

Powołanie administratora bezpieczeństwa informacji

Administrator danych może powołać administratora bezpieczeństwa informacji. W przypadku niepowołania administratora bezpieczeństwa informacji zadania ABI (określone w ustawie) wykonuje administrator danych (art. 36a uodo).

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

Zgodnie z art. 37 RODO administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:

a) przetwarzania dokonują organ lub podmiot publiczny;
b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;
c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych.

W przypadkach innych można wyznaczyć lub jeżeli wymaga tego prawo Unii lub prawo państwa członkowskiego, wyznacza się inspektora ochrony danych.

Wskazówka

Nieduże biuro rachunkowe raczej nie spełni żadnej powyższej przesłanki i nie będzie zobowiązane do wyznaczenia inspektora ochrony danych, czyli wysoce wyspecjalizowanej i wykwalifikowanej osoby zajmującej się głównie nadzorem nad przestrzeganiem zasad i przepisów dotyczących ochrony danych osobowych. Administrator danych, czyli właściciel bądź prezes biura, może wyznaczyć osobę ze swojego personelu, która w imieniu administratora, jako wewnętrzny specjalista ds. ochrony danych lub pełnomocnik zarządu ds. bezpieczeństwa informacji (nazwa ma tu drugorzędne znaczenie) będzie pilnować, aby były spełnione wymagania prawne i organizacyjne zapewniające wysoki poziom ochrony danych. Wzór załącznika wyznaczającego taką osobę i opisujący jej zadania znajduje się na www.dokumentacjaksiegowa.pl. Zarówno obecnie, jak i w przyszłości powołanie ABI czy wyznaczenie DPO (IOD – inspektora ochrony danych) dla większości biur rachunkowych będzie uprawnieniem, a nie obowiązkiem.

Oprócz wyznaczenia specjalisty ds. ochrony danych osobowych warto, a raczej należy mieć administratora systemu informatycznego – ASI , czyli głównego informatyka, który zadba o bezpieczeństwo i ciągłość działania systemu informatycznego, zwłaszcza służącego do przetwarzania danych osobowych. Zadania ASI opisuje załącznik na www.dokumentacjaksiegowa.pl. Administratorem systemu informatycznego może być specjalista zewnętrzny czy zewnętrzna firma informatyczna. Zasady i wytyczne dotyczące bezpieczeństwa teleinformatycznego powinny być zawarte w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Jedną z ważniejszych procedur jest odpowiednie tworzenie, przechowywanie i testowanie zapasowych kopii bezpieczeństwa. ASI powinien wręcz na piśmie przedstawić administratorowi tryb przywracania systemu po jakichkolwiek awariach, w tym katastrofach typu pożar czy powódź.

Zapewnienie kontroli nad danymi

Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane (art. 38 uodo). Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:

1) imię i nazwisko osoby upoważnionej;

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia (art. 39 uodo).

Wskazówka

W rozporządzeniu ogólnym wprawdzie nie ma tak szczegółowych wymogów, niemniej dla formalnego i praktycznego bezpieczeństwa administrator danych musi wiedzieć, który z jego pracowników, jako osoba upoważniona do przetwarzania danych, co i z jakimi informacjami może robić. Zwłaszcza osoby odpowiedzialne za kontakty z instytucjami i podmiotami zewnętrznymi, łącznie z ZUS-em czy US, mające prawo do przekazywania danych, muszą być wyraźnie wskazane i jednocześnie świadome odpowiedzialności za niezgodne z prawem udostępnienie danych. Nadal więc prowadzenie stosownej ewidencji osób upoważnionych do przetwarzania danych jest wskazane. Propozycja wzoru takiej ewidencji znajduje się na www.dokumentacjaksiegowa.pl w zakładce DO POBRANIA.

Wykaz zbiorów danych osobowych

Dokumentacja prowadzona przez administratora danych, opisująca sposób przetwarzania danych oraz podjęte środki dla ich ochrony, ma zawierać między innymi wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, sposób przepływu danych pomiędzy poszczególnymi systemami (rozporządzenie techniczne do ustawy o ochronie danych osobowych.

Zgodnie z art. 30 RODO każdy administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada. W rejestrze tym zamieszcza się wszystkie następujące informacje:

- imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
- cele przetwarzania;
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
- jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
- jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych nie ma zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych.

Wskazówka

Można więc założyć, że małe i średnie biura rachunkowe, jak zacznie obowiązywać RODO, nie będą zobowiązane do prowadzenia żadnego wykazu zbiorów danych czy rejestru czynności przetwarzania danych. Niemniej, aby odpowiednio chronić aktywa i zasoby dotyczące informacji, trzeba wiedzieć, jakie dane posiadamy, w jakich celach i na jakiej podstawie je gromadzimy i wykorzystujemy. Przykładowy więc wykaz zbiorów biura rachunkowego zamieszczony jest na www.dokumentacjaksiegowa.pl. Wskazane tam zbiory są zwolnione z rejestracji u GIODO na podstawie stosownych punktów artykułu 43 ustawy o ochronie danych osobowych.
Wraz ze stosowaniem RODO nie będzie obowiązku zgłaszania żadnych zbiorów danych do następcy prawnego GIODO.

Pojawi się wprawdzie obowiązek oceny skutków dla ochrony danych i uprzednich konsultacji z organem nadzorczym (art. 35 i 36 RODO). Wydaje się jednak mało prawdopodobne, aby nieduże biura rachunkowe objęły takie obowiązki.

Nie ma też i nie będzie żadnego obowiązku przesyłania do GIODO jakichkolwiek regularnych sprawozdań czy planów sprawdzeń. Tego typu pogłoski są zafałszowane.

Pojawi się natomiast obowiązek zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu. W przypadku naruszenia ochrony danych osobowych skutkującym ryzykiem naruszenia praw lub wolności osób fizycznych administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia (art. 33 RODO). Propozycję autorskiego wzoru zgłoszenia naruszenia do organu nadzorczego zamieściliśmy na www.dokumentacjaksiegowa.pl.
W określonych sytuacjach o takim naruszeniu będzie trzeba również powiadomić osobę, której dane zostały naruszone. Niezwłocznie o wszelkich naruszeniach musi informować administratora podmiot przetwarzający.

Piotr Glen
specjalista ds. ochrony danych osobowych

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

BIURO USUWA DANE – JAK, CZYM I KIEDY

Przetwarzanie danych osobowych nie polega wyłącznie na pobieraniu zgód czy powierzaniu przetwarzania innym podmiotom. Również usuwanie przetwarzanych danych, na przykład poprzez niszczenie nośników z danymi, stanowi zagadnienie istotne tak pod względem prawnym, jak i technicznym.

Zgodnie z ustawą z 29 sierpnia 1997 r. o ochronie danych osobowych konieczne jest postępowanie z przetwarzanymi danymi osobowymi w sposób określony w tej ustawie. Z przetwarzaniem danych osobowych mamy do czynienia w przypadku jakiejkolwiek operacji dokonywanej na danych osobowych. Taką operacją jest zgodnie z ustawą na przykład: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie oraz – uwaga – usuwanie tych danych. Nie ma przy tym znaczenia, czy usuwanie odbywa się tradycyjnie (np. przez zniszczenie dokumentu papierowego zawierającego listę klientów biura), czy elektronicznie (np. przez usunięcie pliku z listą klientów biura).

Pod pojęciem usuwania kryje się:

- zniszczenie danych osobowych lub
- modyfikacja danych osobowych, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

Zniszczenie danych osobowych

Chodzi tu o unicestwienie danych osobowych. Ze zniszczeniem danych osobowych mamy do czynienia na przykład w razie takiego fizycznego unicestwienia nośników tych danych, które uniemożliwia odtworzenie informacji na nich zawartych. Zniszczenie danych jest zawsze dokonywane w celu pozbawienia kogokolwiek jakiejkolwiek możliwości dalszego dokonywania jakichkolwiek operacji na tych danych. Ma to więc zapobiec możliwości dalszego przetwarzania danych osobowych.

Dane osobowe a nośnik danych

Istotne w praktyce usuwania danych osobowych jest odróżnianie dwóch pojęć: „dane osobowe” i „nośniki danych”. Ustawodawcy zależy na tym, aby biuro będące administratorem danych osobowych usunęło te dane, a nie sam nośnik. Nośnikami danych, zgodnie ze słownikowym rozumieniem tego pojęcia, są „fizyczne ośrodki przeznaczone do przechowywania danych”. Mogą to być np. dyski twarde, akta, papierowe kartoteki czy pisemne protokoły. Ważne jest, aby zostały usunięte dane, a nie nośnik, więc nie jest usunięciem danych osobowych takie zniszczenie dysku twardego biura, które wprawdzie uniemożliwia korzystanie z tego dysku, ale nie niweczy możliwości odzyskania danych na nim zapisanych.

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

PRZYKŁAD

Załóżmy, że biuro stworzyło listę klientów ze wskazaniem imion i nazwisk lub firm oraz posiadanych przez nich, wybranych cech (np. adres siedziby lub miejsca prowadzonej działalności gospodarczej, wysokość kapitału zakładowego, EBITDA). Jeżeli z listy usuniemy imiona i nazwiska lub firmy poszczególnych klientów, to zmodyfikujemy dane w ten sposób, że nie będziemy mogli już przyporządkować zestawu cech do konkretnej osoby fizycznej będącej naszym klientem.

Ale uwaga – nie zawsze tak będzie.
Załóżmy, że tak okrojoną informację będzie można zestawić z pozyskaną z innego źródła listą imion i nazwisk lub firm naszych klientów, a ponadto, że z tak okrojonej informacji wynika, iż wśród klientów znajduje się tylko jedna osoba prowadząca działalność gospodarczą mająca miejsce prowadzenia działalności w Puławach. Oczywiste będzie, że uda się zidentyfikować tę spółkę i podać jej nazwę.

Mimo więc dokonanej przez nas modyfikacji można, łącznie z innymi informacjami, wskazać na konkretną osobę fizyczną. Modyfikacja nie była tu dokonana w prawidłowy sposób.

Modyfikacja danych osobowych

Drugi ze sposobów usunięcia danych osobowych (czyli ich modyfikacja) to podjęcie takiej czynności w stosunku do danych osobowych, która spowoduje ich anonimizację, która polega na pozbawieniu informacji cech danych osobowych.
Podczas czytania dokumentów w poszukiwaniu miejsc do „zaczernienia" najczęstszym problemem jest właśnie typowanie tych miejsc, a więc określanie, co jest danymi osobowymi, które należy zanonimizować. Pamiętajmy, że:

- dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
- danymi osobowymi nie są informacje, za pomocą których nie da się określić tożsamości osoby bez podjęcia nadmiernych kosztów, czasu lub działań.

Pracownicy biura dokonujący anonimizacji (np. przed przekazaniem dokumentów do archiwum zewnętrznego) mogą to robić na przykład poprzez usunięcie tej części informacji, która ma charakter osobowy (tj. wskazuje na konkretną osobę fizyczną). Celem zawsze musi bowiem być uniemożliwienie połączenia pozostałych informacji z konkretną osobą fizyczną.

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

I tu dochodzimy do różnicy pomiędzy zniszczeniem a modyfikacją danych osobowych – w tym ostatnim przypadku możliwe jest pozostawienie tej części informacji, która tak samodzielnie, jak i łącznie z innymi informacjami nie pozwala już na zidentyfikowanie konkretnej osoby fizycznej.

Usuwanie, zaprzestanie i wstrzymanie przetwarzania

Przepisy niekiedy nakazują administratorowi danych nie usunięcie danych, lecz „zaprzestanie ich przetwarzania". Na przykład w razie wniesienia przez jakąś osobę żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, administrator danych zaprzestaje przetwarzania kwestionowanych danych osobowych albo bez zbędnej zwłoki przekazuje żądanie Generalnemu Inspektorowi, który wydaje stosowną decyzję.
Nierzadko strony umów (np. umowy zawartej przez biuro rachunkowe z kancelarią prawną o powierzenie przetwarzania danych osobowych) same obligują się wzajemnie, na wypadek zaprzestania dalszej współpracy, do usunięcia i zaprzestania przetwarzania danych.
Jeszcze z inną sytuacją mamy do czynienia na gruncie art. 32 ust. 3 ustawy, zgodnie z którym galimatias zwiększa jeszcze art. 32 ust. 1 pkt 6 ustawy, który przyznaje każdej osobie prawo do żądania czasowego lub stałego „wstrzymania" przetwarzania danych osobowych jej dotyczących, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.
O co tutaj chodzi?
W ocenie autora zarówno „wstrzymanie przetwarzania danych osobowych", jak i „zaprzestanie" ich przetwarzania to synonimy. Znaczą one jednak coś zupełnie innego niż „usuwanie" danych osobowych. W przypadku zaprzestania (oraz wstrzymania) przetwarzania danych osobowych administrator danych nie musi ich usuwać ze zbioru danych, ale jest zobowiązany powstrzymać się przed dokonywaniem jakichkolwiek operacji na tych danych. Takie rozumienie trzech analizowanych terminów wydaje się być uzasadnione także podczas interpretowania umów cywilnoprawnych, w których pojęcia te zostały użyte.

Ujęcie usuwania danych w praktyce i regulacjach wewnętrznych

Jak już wiemy, regulacja kwestii usuwania danych osobowych na poziomie ustawowym jest raczej skromna. Oznacza to, że na biurze jako administratorze danych spoczywa obowiązek zapewnienia prawidłowości przebiegu usuwania danych osobowych, przez co należy rozumieć:

- podejmowanie decyzji o usunięciu danych osobowych;
- wybranie sposobu usunięcia danych osobowych (zniszczenie lub modyfikacja);
- wybranie metody zniszczenia lub modyfikacji danych osobowych, w tym postępowania z ich nośnikiem;
- fizyczne wykonanie zniszczenia lub modyfikacji z udokumentowaniem tego zdarzenia.

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

Podejmowanie decyzji o usunięciu danych osobowych

Usunięcie, czyli zarówno zniszczenie, jak i modyfikacja danych osobowych, nie wymagają zgody tej osoby, której dane dotyczą. Mówiąc wprost: biuro może je usunąć w dowolnym momencie i z jakiejkolwiek przyczyny. Do usunięcia danych osobowych nie jest w szczególności konieczne zaistnienie którejkolwiek z przesłanek legalizujących przetwarzanie danych osobowych. Oznacza to, że administrator danych nie musi się zastanawiać, czy np. ich usunięcie jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. W przeciwnym wypadku mogłoby się okazać, że np. biuro nie może sprzedać zużytego komputera, gdyż na uprzednie usunięcie z niego danych osobowych nie zgodził się jakiś klient biura.

Zawsze przed podjęciem decyzji o usunięciu danych należy jednak przeanalizować, czy usunięcie danych jest możliwe w świetle postanowień zawartych umów. Może być bowiem tak, że np. zawarcie umowy z klientem zobowiązuje nas do przetwarzania jego danych osobowych w związku z obsługą finansowo-księgową. Jeżeli więc współpraca z klientem ustaje, to możemy jego dane osobowe usunąć z naszej bazy danych, ale tylko w świetle przepisów dotyczących ochrony danych osobowych. Jeżeli te dane usuniemy, to nie będziemy przecież w stanie prawidłowo zrealizować reklamacji, a tym samym wykonać umowy, co może nas w konsekwencji kosztować konieczność wypłaty odszkodowania. Dlatego prawidłowa kolejność powinna być następująca: rozwiązanie umowy z klientem i usunięcie jego danych – a nie na odwrót.

Wybranie sposobu usunięcia danych osobowych

To, czy w danym przypadku powinno nastąpić zniszczenie, czy też modyfikacja danych osobowych, warto uregulować w wewnętrznych przepisach administratora danych. Chodzi o to, aby przynajmniej w najczęstszych lub najistotniejszych przypadkach osoba upoważniona do przetwarzania danych w imieniu biura nie miała wątpliwości co do sposobu ich zniszczenia. Przykładowy zapis może brzmieć następująco: „Dane osobowe znajdujące się na elektronicznych nośnikach danych niszczone są niezwłocznie po ustaniu celu ich przechowywania. Za zniszczenie danych osobowych odpowiada użytkownik”.
Użyte w powyższym przykładzie słowo „niszczenie” nie odpowiada wprawdzie dokładnie charakterystyce danych osobowych przetwarzanych w formie elektronicznej, przez co może zachęcić użytkownika do zniszczenia nośnika danych, ale jest prawidłowe z prawnego punktu widzenia. Z tego powodu wydaje się zasadne zdefiniowanie w regulacji wewnętrznej zarówno tego, na czym polega zniszczenie i zmodyfikowanie danych przechowywanych tak czy to w formie papierowej, czy elektronicznej.
Wydaje się, że zasadniczo bezpieczniejszym dla administratora danych (a co za tym idzie – domyślnym) rozwiązaniem powinno być niszczenie danych.

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

Metoda niszczenia lub modyfikacji danych i jej dokumentowanie

Między innymi brytyjski odpowiednik polskiego GIODO zauważył, że całkowite usunięcie danych osobowych z systemów informatycznych nie zawsze jest możliwe. Chodzi tu chociażby o takie sytuacje jak uprzednie kopiowanie danych osobowych w ramach kopii zapasowych systemu czy przechowywanie danych osobowych połączonych z innymi danymi w ten sposób, że nie jest możliwe precyzyjne wydzielenie danych osobowych i ich zniszczenie, a zniszczenie całego zbioru danych nie wchodzi w rachubę. Z tych powodów należy zalecić, aby administrator danych przynajmniej:

- zrobił wszystko, co może, aby usunąć dane osobowe z możliwie każdej lokalizacji, w jakiej zostały utrwalone, bez usuwania innych danych;
- powstrzymał się od jakiegokolwiek przetwarzania danych osobowych pozostawionych np. w formie kopii zapasowej, z której danych tych nie da się usunąć bez poważnego nakładu sił i środków.

Usunięcie danych może także polegać na zniszczeniu nośnika tych danych razem z samymi danymi. Tak będzie najczęściej w przypadku przechowywania danych osobowych w tradycyjnej formie pisemnej. Wymóg zniszczenia danych osobowych spełnia „przepuszczenie" dokumentu przez niszczarkę lub jego spalenie.
Samo usuwanie danych osobowych lub ich modyfikowanie może być dokonywane okresowo, jeżeli nie jest wymagalne natychmiastowe zniszczenie danych osobowych. Wówczas dla zniszczenia większej partii danych można powołać komisję. Niezależnie od tego, czy dane są niszczone komisyjnie, czy „na bieżąco" przez osobę dopuszczoną przez administratora danych do ich przetwarzania, ze zniszczenia danych powinien pozostać jakiś ślad. Może to być np. log komputerowy wskazujący na dokładny czas usunięcia danych i osobę, która dane usunęła. W przypadku działań komisji warto pokusić się o formę protokołu, w którym zostaną wskazane:

- rodzaj i nazwa zbioru usuwanych danych;
- podstawa prawna usunięcia danych osobowych ze zbioru danych (można tu wskazać także np. wewnętrzną regulację);
- opis usuniętych danych osobowych;
- skład komisji usuwającej dane osobowe;
- opis sposobu usunięcia danych osobowych;
- datę i miejsce usunięcia danych osobowych;
- podpisy członków komisji.

Protokół powinien być przechowywany przez administratora danych osobowych lub administratora bezpieczeństwa informacji na potrzeby ewentualnej kontroli przeprowadzonej przez inspektorów Biura Generalnego Inspektora Ochrony Danych Osobowych.

Marcin Sarna
radca prawny

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

PODMIOTY OBSŁUGUJĄCE BIURO A DANE OSOBOWE BIURA. CZY I JAK JE UDOSTĘPNIAĆ?

W praktyce działalności biur często dochodzi do sytuacji, w których dane osobowe przetwarzane przez to biuro muszą być udostępnione innym podmiotom. Prawo dopuszcza taką możliwość, ale pod pewnymi warunkami, przedstawionymi w tym artykule.

W przypadku gdy podmiot inny niż biuro chce (musi) korzystać z danych osobowych, dla których biuro jest administratorem, to w zasadzie zawsze będziemy mieli do czynienia z przetwarzaniem tych danych przez ów inny podmiot. Definicja przetwarzania jest bowiem bardzo szeroka i obejmuje jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. Oznacza to w praktyce, że administrator danych zawsze musi udostępnić dane osobowe w jeden z dwóch sposobów przewidzianych prawem.

Sposoby udostępnienia danych osobowych odbiorcy danych

Podmiot, któremu biuro udostępnia dane osobowe, jest w rozumieniu ustawy odbiorcą danych. Do takiego udostępnienia może dojść na jeden z dwóch sposobów:

- poprzez powierzenie przetwarzania danych osobowych;
- poprzez sprzedaż bazy danych osobowych podmiotowi trzeciemu (najczęściej nazywa się to właśnie udostępnieniem danych osobowych).

Powierzenie przetwarzania danych osobowych

Biuro jako administrator danych osobowych może zawrzeć pisemną umowę z innym podmiotem, na mocy której powierzy temu podmiotowi przetwarzanie danych osobowych. Przetwarzanie to może się odbywać wyłącznie w celu i w zakresie przewidzianym w umowie.
Przed rozpoczęciem przetwarzania powierzonych mu danych podmiot musi zastosować środki zabezpieczające zbiór danych. Chodzi tu o spełnienie wymagań z art. 36–39 ustawy, tj. w szczególności:

- zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;
- ewentualnie – powołanie administratora bezpieczeństwa informacji;
- zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

Jeżeli dane osobowe są przetwarzane z wykorzystaniem systemów informatycznych, to podmiot, któremu dane się powierza, musi także spełniać wymagania określone w rozporządzeniu ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Na podmiocie przetwarzającym powierzone mu dane ciąży dokładnie taka sama odpowiedzialność za ich przetwarzanie jak na administratorze danych (biurze). Powierzenie mu przetwarzania danych nie czyni go jednak jeszcze administratorem danych, co oznacza zwolnienie go np. z obowiązku rejestracji bazy danych.

Udostępnienie danych osobowych

O ile dane osobowe powierza się do przetwarzania innemu podmiotowi tylko w określonym celu (i często jedynie na pewien czas), o tyle sprzedaż bazy danych osobowych to całkowita zmiana celu wykorzystywania danych osobowych i zupełne przekazanie danych osobowych innemu podmiotowi.

Biuro sprzedające dane osobowe musi być do tego uprawnione, tj. musi posiadać zgodę osób, których dane są przetwarzane, na udostępnienie lub sprzedaż tych danych innemu podmiotowi. Podmiot ten musi być dokładnie określony w treści samej zgody.

Oznacza to, że przed sprzedażą danych osobowych (a w zasadzie nawet jeszcze na etapie sporządzania oferty takiej sprzedaży) biuro powinno przefiltrować bazę i usunąć z niej te dane, co do których nie uzyskało ono zgody na sprzedaż potencjalnemu kupującemu. Pozostawienie danych osób, których zgody nie pozyskano, jest możliwe jedynie w przypadku gdy zachodzi któraś z sytuacji enumeratywnie wyliczonych w art. 23 ust. 1 pkt 2–5 ustawy o ochronie danych osobowych (np. jest to konieczne do realizacji umowy).

Kupujący bazę danych osobowych musi poinformować osoby, których dane zakupił, o:

- swoim adresie,
- celu i zakresie zbierania danych,
- źródle danych (od kogo je zakupił),
- prawie wglądu do danych i ich poprawiania,
- prawie żądania zaprzestania przetwarzania danych osobowych.

Na kupującym ciążą naturalnie wszystkie obowiązki, jakie ustawa nakłada na administratorów danych osobowych.

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

Kiedy udostępnienie, a kiedy powierzenie przetwarzania?

Wybór pomiędzy właściwą formą przepływu danych osobowych a odrębnymi podmiotami prawa nastręcza niekiedy poważnych trudności.

Ważne jest, aby podejmując decyzję o wyborze między tymi dwiema formami, pamiętać, że firma, której przetwarzanie danych osobowych powierzono, nie może wykorzystywać ich do promowania własnych produktów czy usług. Art. 23 ust. 5 w związku z art. 23 ust. 4 pkt 1 ustawy pozwala bowiem na prowadzenie tzw. marketingu bezpośredniego własnych produktów lub usług administratora danych, ale już nie na marketing produktów czy usług podmiotu, któremu administrator danych je powierzył.

Współodpowiedzialność za bezpieczeństwo danych

Problem z ochroną danych osobowych w praktyce polega m.in. na tym, że bardziej świadomi swoich obowiązków administratorzy danych spotykają się z niezrozumieniem podmiotów, których kultura ochrony danych jest na niższym stopniu rozwoju. Problem ten dotyczy także samych administratorów danych, w tym biur rachunkowych.

PRZYKŁAD

ABCOM sp. z o.o. zawarła z Biurem Rewizorów Auditax sp. z o.o. umowę na przeprowadzenie audytu bezpieczeństwa systemu informatycznego i wdrożenie wniosków z tego audytu w życie. W toku prac audytowych okazało się, że do przeprowadzenia audytu konieczne będzie zmigrowanie bazy danych zawierającej dane osobowe i w związku z tym ABCOM sp. z o.o. będzie je przetwarzała. Spółka informatyczna zaproponowała więc zawarcie umowy o powierzeniu przetwarzania danych osobowych, ale biuro rachunkowe uznało, że nie ma takiej potrzeby. Impas w tej kwestii spowodował ostatecznie, że audyt zamiast ABCOM sp. z o.o. dokończył inny, mniej „wymagający", podmiot.
Takie działanie biura trudno uznać za prawidłowe.

Współpracujące ze sobą firmy często nie rozumieją, że są współodpowiedzialne za dane osobowe, które przetwarzają. Zawarcie umowy regulującej zasady udostępnienia danych (czy to przez sprzedaż bazy danych, czy też powierzenie ich przetwarzania) jest w interesie każdego z tych podmiotów:

- odbiorca danych dzięki umowie ma podstawę prawną ich przetwarzania (nie naraża się na zarzut bezprawnego przetwarzania danych);
- biuro udostępniające dane zyskuje drugi, współodpowiedzialny podmiot za przetwarzanie danych osobowych (przy powierzeniu przetwarzania) oraz czyni to na podstawie legalnej przesłanki udostępniania danych.

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

Słowo „współodpowiedzialny" oznacza, że biuro odpowiada za bezpieczeństwo danych powierzonych do przetwarzania innemu podmiotowi. Powinno sobie w związku z tym zapewnić w umowie możliwość kontroli przetwarzania tych danych.
Nie bez znaczenia są także względy PR-owe: podmioty należycie chroniące dane osobowe są za to doceniane przez swoich klientów.

UWAGA

Udostępnianie danych osobowych ma także inne znaczenie niż to, o którym piszemy w artykule 29 ustawy o ochronie danych osobowych, nakazuje, na żądanie uprawnionych organów, udostępnić im dane osobowe, jeżeli organy te uzasadnią potrzebę ich posiadania oraz wskażą m.in. zakres i przeznaczenie tych danych.

Przesłanki udostępniania danych osobowych

Jak zauważyliśmy na wstępie, udostępnianie danych osobowych jest jednym z przejawów (rodzajów) ich przetwarzania. Oznacza to, że aby administrator danych mógł je udostępnić innemu podmiotowi, musi zajść jedna z przesłanek przetwarzania danych określonych w art. 23 ustawy. Jednocześnie jednak należy pamiętać, że nie mogą zajść przesłanki negatywne, np. dane osobowe są dodatkowo chronione jako tajemnica państwowa lub zawodowa.

Podczas szukania w art. 23 podstawy do przekazania danych główną pokusą jest powołanie się – w braku osobnej zgody podmiotu, którego dane są przetwarzane – na to, że udostępnienie danych jest „niezbędne do wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą" (art. 23 ust. 1 pkt 5). Ta tzw. przesłanka prawnie usprawiedliwionego celu bywa niestety interpretowana nazbyt szeroko. Jeżeli biuro ma wątpliwości, czy dane udostępnienie odbywa się w ramach prawnie usprawiedliwionego celu, powinno jednak poprosić o zgodę podmiot, którego dane są przetwarzane.

Sankcje

Zgodnie z art. 51 ustawy o ochronie danych osobowych osoba, która administrując zbiorem danych lub będąc obowiązana do ochrony danych osobowych, udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. W przypadku nieumyślności tego czynu jest on penalizowany grzywną, karą ograniczenia wolności albo pozbawienia wolności od roku.

Marcin Sarna
radca prawny

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

NOWA TWARZ W BIURZE – OBOWIĄZEK USTANOWIENIA INSPEKTORA OCHRONY DANYCH ZGODNY Z RODO

Rozporządzenie europejskie w sprawie ochrony danych osobowych (tzw. RODO) zmieni sposób ochrony danych osobowych także w Twoim biurze rachunkowym. Jednym z obszarów, w których zajdą zmiany, jest administrator bezpieczeństwa informacji. Przeczytaj artykuł, aby dowiedzieć się, co się stanie z ABI w maju 2018 roku oraz czy będziesz musiał ustanowić inspektora ochrony danych.

RODO będzie bezpośrednio stosowane w państwach członkowskich od 25 maja 2018 r. Warto jednak już dziś zacząć przygotowywać się do wprowadzanych nim zmian. Rozporządzenie to nie posługuje się terminem „administrator bezpieczeństwa informacji". Zamiast niego system ochrony danych osobowych wzbogaci się o inspektora ochrony danych, który ma przejąć prawa i obowiązki dotychczasowego ABI. Podobieństwo nazwy „inspektor ochrony danych osobowych" do ochrony informacji niejawnych wskazuje nam na pewną tendencję – coraz większy rygoryzm ochrony danych osobowych zbliżający ten system właśnie do ochrony informacji niejawnych.

Inspektor niejedno ma imię

Preambuła rozporządzenia wskazuje, że podmioty tzw. sektora prywatnego (a więc także biura rachunkowe) przetwarzający dane osobowe są administratorami danych osobowych. Administrator obecnie wykonuje swoje obowiązki z pomocą ABI, a będzie – z pomocą inspektora ochrony danych. Inspektor powinien mieć zapewnioną przez administratora danych możliwość wykonywania swoich zadań w sposób niezależny od tego administratora.

WAŻNE

Od tego inspektora należy odróżnić Europejskiego Inspektora Ochrony Danych, który będzie wchodził, obok szefów organów naczelnych państw członkowskich, w skład Europejskiej Rady Ochrony Danych. Nie ma on nic wspólnego z inspektorami ochrony danych u poszczególnych administratorów danych osobowych.

ADO wyznacza inspektora ochrony danych

To administrator danych osobowych wyznacza inspektora ochrony danych. Podobnie jak dziś ustanowienie ABI, także ustanowienie inspektora nie jest zasadniczo obowiązkowe. Obowiązek jego powołania będzie ciążył m.in. na tym biurze rachunkowym:

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

- którego główna działalność polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;
- którego główna działalność polega na przetwarzaniu na dużą skalę danych osobowych.

Czyli generalnie, o ile administrator bezpieczeństwa informacji mógł, ale nie musiał być wyznaczony (a wówczas musiał być zgłoszony do GIODO), o tyle w przypadku nowego inspektora ochrony danych jego istnienie jest obowiązkowe w zasadzie zawsze, gdy wskazuje na to: kategoria przetwarzanych danych, cel przetwarzania danych na dużą skalę albo gdy mówimy o jednostce publicznej. Biorąc pod uwagę tak sformułowane przesłanki ustanowienia inspektora ochrony danych osobowych, biura rachunkowe w większości będą musiały go powołać.W pozostałych przypadkach wyznaczenie inspektora ochrony danych jest fakultatywne.

WAŻNE

Zgłoszenie inspektora danych do organu nadzorczego jest obowiązkowe, więc tutaj zmiany *de facto* nie ma i biuro będzie musiało zgłosić inspektora danych do prezesa Urzędu Ochrony Danych Osobowych, który zastąpi obecnego Generalnego Inspektora Ochrony Danych Osobowych.

Będzie także istniała możliwość powołania jednego wspólnego inspektora ochrony danych dla:

- grupy przedsiębiorstw – jeżeli można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej;
- kilku organów lub podmiotów publicznych – z uwzględnieniem ich struktury organizacyjnej i wielkości;
- zrzeszeń lub innych podmiotów reprezentujących określone kategorie administratorów.

Kto na inspektora?

Wyznaczenie inspektora powinno się odbyć na podstawie kwalifikacji zawodowych. Chodzi tu w szczególności o wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętność wypełnienia zadań inspektora.

Inspektor ochrony danych może być członkiem personelu administratora danych osobowych (czyli pracownikiem albo osobą współpracującą z biurem rachunkowym na podstawie umowy cywilnoprawnej, np. umowy o świadczenie usług). Jego dane muszą być opublikowane przez administratora.

Obowiązki biura rachunkowego względem swojego inspektora

Biuro będzie musiało:

- zapewnić, aby inspektor był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

- wspierać inspektora w wypełnianiu przez niego jego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej;
- zapewnić, aby inspektor nie otrzymywał instrukcji dotyczących wykonywania jego zadań.

Szefostwo biura nie będzie mogło:

- odwołać ani ukarać inspektora za wykonywanie przez niego zadań, ale tylko tak długo, jak długo inspektor działa w granicach i na podstawie rozporządzenia;
- zabronić osobie, której dane osobowe dotyczą, kontaktu bezpośrednio z inspektorem we wszystkich sprawach związanych z przetwarzaniem tych danych oraz z wykonywaniem praw przysługujących tym osobom.

Dane inspektora

W przypadku gdy biuro zbiera dane osobowe danej osoby, właśnie od niej wówczas biuro jako ADO będzie zobowiązane podać tej osobie m.in. dane kontaktowe inspektora ochrony danych. Czyli na przykład jeżeli biuro dostało dane Jana Kowalskiego od swojego klienta, który zawarł z Janem Kowalskim jakąś umowę, to wówczas biuro nie musi Janowi Kowalskiemu przekazywać danych kontaktowych inspektora ochrony danych.
Ponadto istnieje także generalny obowiązek opublikowania danych kontaktowych administratora (art. 37 ust. 7 rozporządzenia). Biuro może temu obowiązkowi zadośćuczynić, umieszczając te dane kontaktowe na swojej stronie internetowej.

Obowiązki inspektora

Do zadań inspektora ochrony danych należą:

- informowanie biura (administratora danych osobowych) oraz pracowników biura, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
- monitorowanie przestrzegania przepisów o ochronie danych oraz polityk biura, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu biura uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania; z żądaniem tym może wystąpić zarówno samo biuro (kierownictwo, zarząd), jak i – w ocenie autora – poszczególni pracownicy biura;
- współpraca z organem nadzorczym (prezesem UODO, który zastąpi obecnego GIODO);

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych – jeżeli prezes UODO będzie chciał się kontaktować z biurem rachunkowym w sprawie ochrony danych osobowych, to gros korespondencji będzie spływało bezpośrednio do inspektora ochrony danych, a nie do kierownictwa biura.

Zadania te powinny być wypełniane z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

Zadania inspektora muszą być także określone w wiążących regułach korporacyjnych, jeżeli w danym biurze zostaną one przyjęte (w praktyce będzie to zapewne dotyczyło wyłącznie biur funkcjonujących w ramach struktur grupy kapitałowej).

Powyższe obowiązki nie stanowią wszystkich obowiązków, jakie może mieć inspektor ochrony danych w danym biurze. Wykonywanie funkcji inspektora ochrony danych przez daną osobę nie ogranicza bowiem kierownictwa biura rachunkowego w możliwości zlecania inspektorowi także innych zadań i obowiązków, jeżeli tylko nie powodują one konfliktu interesów. Takim przykładem na konflikt interesów może być np. powierzenie inspektorowi ochrony danych przetwarzania danych osobowych klientów biura we własnych celach marketingowych biura, czyli po prostu nakazanie mu wykonywania funkcji reklamowych.

Inspektor w podmiocie przetwarzającym

Rozporządzenie przewiduje, że inspektor ochrony danych powinien zostać wyznaczony nie tylko u administratora danych osobowych, ale także w tzw. podmiocie przetwarzającym. Jest to w zasadzie obecny procesor z art. 31 ustawy o ochronie danych osobowych, a więc podmiot, któremu administrator danych osobowych powierzył ich przetwarzanie.

Co to oznacza dla biura rachunkowego? Jak już wiemy, na mocy nowych przepisów biuro raczej będzie musiało ustanowić inspektora ochrony danych. Nie ma więc znaczenia, czy biuro dodatkowo przetwarza dane osobowe powierzone mu np. na mocy umowy zawartej z klientem. Biuro musi jednak mieć na uwadze, że podmiot, któremu to biuro dane przekazuje, a więc podmiot przetwarzający, powinien posiadać ustanowionego inspektora ochrony danych. Należy zalecić, aby biuro dopilnowało, by w umowie o powierzeniu przetwarzania danych osobowych podmiotowi trzeciemu zawarte zostało zapewnienie tego podmiotu o posiadaniu przez niego prawidłowo ustanowionego i kompetentnego inspektora ochrony danych.

Dlaczego jest to takie ważne? Jak wskazuje pkt 81 preambuły do rozporządzenia, administrator powinien, powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

– w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania. W ocenie, czy dany podmiot przetwarzający zapewnia te gwarancje, będzie więc miało znaczenie także i to, jaką fachowość prezentuje inspektor ochrony danych zaangażowany przez ten podmiot przetwarzający.

Sankcja za brak inspektora

Naruszenie przepisów dotyczących obowiązków administratora i podmiotu przetwarzającego podlega zgodnie administracyjnej karze pieniężnej w wysokości do 10.000.000 euro, a w przypadku przedsiębiorstw nawet do 2% całkowitego rocznego obrotu przedsiębiorstwa z poprzedniego roku obrotowego (jeżeli te 2% wynosi mniej niż 10.000.000 euro, to w dalszym ciągu można nałożyć na przedsiębiorstwo karę do 10.000.000 euro). Bez wątpienia jednym z takich penalizowanych obowiązków biura jest ustanowienie inspektora ochrony danych.
Ustalając, czy kara w ogóle powinna być nałożona, a także jaki powinien być jej wymiar, organ powinien wziąć pod uwagę m.in.:

- charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody;
- działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;
- wszelkie wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego.

WAŻNE

Zwróć uwagę na zmieniony sposób nakładania kary. Obecnie GIODO, aby nałożyć karę, musi najpierw wezwać podmiot przetwarzający dane do usunięcia naruszenia prawa. Po zmianach GIODO nałoży karę bez takiego uprzedniego wezwania.

Zostało mało czasu

Pamiętajmy, że do czasu wprowadzenia nowych zasad odnoszących się do „oficera bezpieczeństwa danych osobowych" w Twoim biurze rachunkowym pozostało już niewiele ponad pół roku. Polski ustawodawca będzie musiał w tym czasie zmienić polskie regulacje dotyczące ochrony danych osobowych – już trwają prace legislacyjne nad nową ustawą o ochronie danych osobowych. Ta sytuacja wymaga od kierownictwa biura rachunkowego monitorowania stanu prawnego, jaki ich zastanie po 25 maja 2018 r.

W wieloletnich umowach o współpracę, w których kwestia danych osobowych jest poruszana (np. jedna ze stron powierza drugiej stronie przetwarzanie danych osobowych), warto obok

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

administratora bezpieczeństwa informacji dopisywać np. taki zwrot: „lub inspektora ochrony danych". Jeżeli w regulacjach wewnętrznych biura zamieszczane są odniesienia do administratora bezpieczeństwa informacji, to warto rozważyć zdefiniowanie go jako także „inspektora ochrony danych" lub „wspólnego inspektora ochrony danych" – przez objęcie wszystkich tych „strażników danych" jedną definicją. Pozwoli to na prawidłowe przygotowanie terminologiczne aktów wewnętrznych.

Wreszcie już teraz, jeżeli nie uczyniono tego do tej pory, można upublicznić dane kontaktowe obecnego administratora bezpieczeństwa informacji przez podanie ich na stronie organizacji oraz informować o tych danych w klauzulach informacyjnych.

Nie bez znaczenia może być także zwiększenie popytu na usługi obecnych administratorów bezpieczeństwa informacji. Nie można przecież całkowicie wykluczyć niedostatku wykwalifikowanych inspektorów ochrony danych w początkowym okresie obowiązywania nowych regulacji, skoro tak drastycznie zwiększy się zakres administratorów danych zobowiązanych do zatrudnienia inspektora ochrony danych. Z tego powodu warto rozważyć zatrudnienie lub rozpoczęcie szkolenia osoby, która obejmie obowiązki ABI, a w przyszłości inspektora ochrony danych.

§ Podstawa prawna:

- ogólne rozporządzenie o ochronie danych osobowych (RODO), tj. rozporządzenie Parlamentu Europejskiego i Rady z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

Marcin Sarna
radca prawny

FabrykaWiedzy.com
Fachowe publikacje dla specjalistów
Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

BIURO RACHUNKOWE

w praktyce

Numer 11
Październik 2017
ISSN 2543-4918
Zadaj pytanie naszym ekspertom
biurorachunkowe@wip.pl
BIURO RACHUNKOWE
w praktyce
RÓŻNE FORMY ROZLICZEŃ PODATNIKÓW • DORADZTWO DLA KLIENTA
ZARZĄDZANIE BIUREM • ROZWÓJ ZAWODOWY
Wskaźnik zysku na akcje. Poznaj zasady jego wyliczania
Twoje biuro może wykorzystać nową aplikację do wysyłania plików JPK
Bilans 2017. Sprawdź, które zmiany w ustawie o rachunkowości należy w nim uwzględnić
Poznaj zasady ubiegania się o kwalifikacje biegłego rewidenta po zmianie przepisów
RODO. Już wkrótce zacznie obowiązywać nowy system sankcji
FICYNA FK.
NOWOŚĆ NA RYNKU WYDAWNICZYM
Jedyny na rynku magazyn wyłącznie dla Biur Rachunkowych
Czym zajmuje się Biuro Rachunko
Czym zajmuje się Biuro Rachunkowe XXI wieku?
Przepis na sukces Biura Rachunkowego

Starannie wyselekcjonowane informacje dla właścicieli Biur Rachunkowych

PRZETESTUJ za 0 zł

- ✔ zagadnienia podatkowo-rachunkowe z uwzględnieniem różnych form rozliczeń podatników (pełne księgi, PKPIR, ryczałt);
- ✔ sprawozdania i raporty;
- ✔ informacje pomocne w doradztwie dla klienta;
- ✔ zagadnienia z prawa handlowego, cywilnego, prawa pracy;
- ✔ przetwarzanie i ochrona danych osobowych;
- ✔ promocja i reklama, współpraca z klientami, odpowiedzialność, zarządzanie biurem rachunkowym;
- ✔ materiały niezbędne do podnoszenia kwalifikacji zawodowych pracowników biura.

Zamów bezpłatny egzemplarz

Masz pytania? Skontaktuj się z naszym Centrum Obsługi Klienta: tel. 22 518 29 29, email: cok@wip.pl, biurorachunkowe@wip.pl

Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131

FICYNA FK.
FINANSOWO-KSIĘGOWA

Więcej ebooków
o tematyce finansowo-księgowej:
www.fabrykawiedzy.com

1FS0016
ISBN: 978-83-269-6786-3

WIEDZA i PRAKTYKA
20 lat

Plik zabezpieczony watermarkiem jawnym i niejawnym: 7151703A30663131